

Acceptable Use Policy

Ongo Agility / Responsible, controlled and permitted use

Version 2026–27 / Updated 8 September 2026

Draft for legal review. Prepared for Ongo Systems B.V. This document should be reviewed by Dutch legal counsel before first external use and read together with the Master Service Agreement, applicable Order Form and, where applicable, the DPA, SLA and regulatory addenda.

This Acceptable Use Policy ("AUP") forms part of the Agreement governing the use of Ongo Agility and the related Services. It applies to Customer, Authorized Users, and any person or system using the Services through Customer's Account, credentials, integrations or instructions. Capitalized terms not defined in this AUP have the meanings given in the Master Service Agreement ("MSA"). Customer is responsible for ensuring that use under its control complies with this AUP.

1. Purpose and core principle

1.1 Ongo Agility is designed to support controlled operational workflows, coordination, decision support and execution by connecting work, people, permissions, systems and AI-enabled capabilities within Customer-defined authority.

1.2 Customer shall configure and use the Services with appropriate governance, permissions, approval steps,

human oversight and escalation paths for the relevant use case, taking account of applicable law, Customer policy and the foreseeable consequences of error or misuse.

1.3 Each Party remains responsible for the obligations that apply to its own role under applicable law.

Nothing in this AUP transfers to Customer an obligation that applies to Ongo as provider, processor or other regulated operator, or transfers to Ongo an obligation that applies to Customer as controller, deployer, employer, professional decision-maker or other regulated operator.

2. General prohibited use

2.1 Customer shall not use the Services, or permit them to be used, to:

(a) violate applicable law, regulation, sanctions, export-control requirements, court orders or binding governmental requirements; **(b)** infringe, misappropriate or unlawfully disclose intellectual property, privacy, confidentiality, publicity or

other third-party rights; **(c)** introduce malware, malicious code, destructive payloads, ransomware, credential theft, phishing,

unauthorised surveillance or other harmful technical activity; **(d)** gain or attempt to gain unauthorised access to systems, accounts, networks, data or facilities, or materially

interfere with the security, integrity, performance or availability of any service; (e) commit or facilitate fraud, unlawful deception, impersonation, forgery, coercion, harassment, threats,

abuse or other unlawful conduct; (f) send or facilitate unlawful unsolicited communications, phishing, deceptive solicitations or

communications that falsely represent their source, authority or purpose; (g) cause or facilitate unlawful discrimination, or make unlawful decisions concerning individuals based on

protected or sensitive characteristics; (h) generate, manipulate, distribute or facilitate child sexual abuse material, or sexually explicit or intimate

material concerning an identifiable person without the consent required by applicable law; (i) circumvent or defeat usage limits, security controls, access controls, approval gates, audit functions,

licensing restrictions, model-routing restrictions or other technical safeguards;

(j) systematically extract Ongo proprietary technology, non-public prompts, system behaviour, configuration,

outputs or other protected material for the purpose of replicating, reverse engineering or training a competing service, except to the extent a restriction is prohibited by mandatory law; (k) submit, connect, disclose or otherwise process data for which Customer lacks the rights, permissions,

legal basis or authority required for the intended processing; or (l) instruct an agent, integration, automation or other system to perform an action that Customer itself would

be prohibited from performing under the Agreement.

3. Prohibited AI practices

3.1 Customer shall not use the Services for an AI practice that is prohibited under applicable law. Where the

EU Artificial Intelligence Act (Regulation (EU) 2024/1689, as amended) applies, this includes any prohibited practice within Article 5, subject to the scope, definitions and lawful exceptions in force at the relevant time.

3.2 Without limiting Section 3.1, Customer shall not use the Services, where prohibited by applicable law or outside an applicable legal exception, to:

(a) use subliminal, purposefully manipulative or deceptive techniques, or exploit vulnerabilities linked to age,

disability or a specific social or economic situation, in a manner that materially distorts behaviour and causes or is reasonably likely to cause significant harm; (b) perform social scoring that results in detrimental, unfavourable, unjustified or disproportionate treatment

of individuals or groups; (c) assess or predict an individual's risk of committing a criminal offence solely from profiling, personality

traits or characteristics; (d) create or expand facial-recognition databases through untargeted scraping of facial images from the

internet, CCTV or comparable sources; (e) infer emotions in the workplace or in education settings where such use is prohibited; (f) use biometric categorisation to deduce or infer sensitive or protected characteristics where prohibited; (g) conduct real-time remote biometric identification in publicly accessible spaces for law-enforcement

purposes outside the strict conditions, authorisations and safeguards permitted by applicable law; or (h) generate or manipulate non-consensual intimate material or material involving the sexual abuse or

exploitation of children. 3.3 The examples in Section 3.2 are not exhaustive. Regulatory classifications, exceptions and application

dates are determined by applicable law as in force from time to time.

4. High-impact and regulated uses

4.1 Customer shall not deploy the Services for a use that may produce legal or similarly significant effects on an individual, materially affect access to rights or essential services, or control a safety-critical function unless the use is expressly within the agreed scope and the required governance and safeguards have been documented.

4.2 Regulated or high-impact contexts may include employment and worker management; education and examinations; access to essential public or private services; credit, lending or insurance; healthcare diagnosis or treatment; biometrics; critical infrastructure; law enforcement; migration, asylum or border control; legal services; public-sector decision-making; and other contexts designated by applicable law.

4.3 Before deployment of a regulated or high-impact use, Customer shall determine the legal and internal requirements applicable to its role and, where required, complete and maintain appropriate impact assessments, notices, consultations, approvals, human-oversight arrangements, monitoring, records and escalation procedures. Ongo may require the use to be described in an Order Form or regulatory addendum and may require reasonable evidence that agreed safeguards are in place.

4.4 Approval or inclusion of a use case in an Order Form confirms contractual scope only. It does not constitute legal advice, regulatory classification, certification of lawfulness or an assumption by Ongo of Customer's statutory or professional responsibilities.

5. Human oversight and authority boundaries

5.1 Customer shall define and maintain appropriate permissions, approval thresholds, transaction or action limits, escalation paths and authority boundaries before enabling AI-enabled actions, automations or agents.

5.2 Customer shall not intentionally bypass a required human approval, safety control, audit mechanism or authority boundary configured for a workflow.

5.3 Unless the applicable Order Form expressly authorises a controlled use with agreed safeguards, AI-enabled functionality shall not be relied upon as the sole basis for an irreversible, safety-critical or legally determinative action.

5.4 Where the Services are configured to initiate or prepare actions involving payments or financial

transfers, execution of contracts or legal filings, employment decisions, benefits or eligibility decisions, medical or safety decisions, destructive data or system changes, or other actions with material external consequences, Customer shall apply approval and verification controls proportionate to the risk and authority involved.

5.5 Customer shall review Outputs and automated actions to the extent required by the use case, applicable

law, Customer policy or risk profile, recognising that AI-enabled functionality may produce incomplete, inaccurate or unexpected results.

6. Transparency, AI literacy and user-facing AI

6.1 Customer shall provide notices and disclosures required by applicable law when individuals interact directly with AI or are exposed to AI-generated or manipulated content through a Customer-controlled use of the Services.

6.2 Where Customer publishes or communicates AI-generated or manipulated content, including deepfakes

or text on matters of public interest, Customer shall comply with applicable labelling, disclosure and editorial-responsibility requirements.

6.3 Where the Services provide configurable transparency, disclosure or labelling mechanisms for Customer-controlled use, Customer is responsible for enabling and configuring them as required for the intended deployment. Ongo remains responsible for provider-side transparency, marking or technical obligations that apply to Ongo by law.

6.4 Each Party shall take reasonable measures to ensure an appropriate level of AI literacy among its own personnel and other persons operating or supervising AI systems on its behalf, taking account of their role, experience, training and the context in which the Services are used.

7. Data, privacy and sensitive information

7.1 Customer shall use only Customer Data and Inputs that it is authorised to process for the intended purpose and shall comply with the DPA, applicable data-protection law and its own retention, access-control and records-management obligations.

7.2 Special-category Personal Data, criminal-offence data, data concerning minors, biometric data and other

highly sensitive information may be processed only where the relevant use is within the agreed scope, Customer has established the required legal basis or other authority, and appropriate contractual, organisational and technical safeguards are in place.

7.3 Customer shall apply data minimisation and shall not use the Services to unlawfully monitor, profile, infer or exploit sensitive attributes or vulnerabilities of individuals.

7.4 Customer shall not use inaccurate, unlawfully obtained or materially inappropriate data in a manner that

creates a foreseeable risk of unlawful or materially harmful decisions about individuals.

8. AI models, integrations and Third-Party Systems

8.1 Customer shall not deliberately route Customer Data to an unapproved external model, plugin, connector, API or Third-Party System through the Services, including through customer-controlled MCP connections, credentials or integrations.

8.2 Customer is responsible for Customer-controlled credentials, accounts, permissions and contractual rights for Customer-selected Third-Party Systems, except to the extent the Order Form states otherwise.

8.3 Customer shall not alter routing, security, model or integration settings in order to circumvent the agreed

deployment architecture, DPA, security configuration or Customer-approved data boundary.

8.4 Ongo may block, disable or isolate an integration, model route, credential or connected system where reasonably necessary to address a material security, legal, privacy or operational risk.

9. Security, testing and platform integrity

9.1 Customer shall protect credentials, API keys, access tokens and other authentication information, shall not share user accounts except where technically intended, and shall use role-based permissions and least privilege appropriate to the use case.

9.2 Customer shall promptly report suspected unauthorised access, material security issues, abuse or unlawful use through the security or legal contact identified in the Order Form or Documentation.

9.3 Customer shall not conduct or permit load testing, penetration testing, vulnerability scanning, adversarial

testing or security research against production systems without Ongo's prior written authorisation, except where the Agreement expressly permits such testing or mandatory law provides otherwise.

9.4 Customer shall not disable, falsify, erase or materially interfere with audit records, security logs or other

evidence controls except through authorised retention or administrative functions.

9.5 Customer shall not use the Services in a manner that imposes excessive or abusive resource consumption, materially degrades service for others, or intentionally defeats reasonable rate, capacity or technical limits.

10. Customer governance and operational controls

10.1 Customer shall identify accountable owners for material workflows and shall ensure that permissions, approval paths and connected-system access remain appropriate as roles, use cases and integrations change.

10.2 Customer shall use the Services in accordance with its own internal policies and authorisations, including any requirements concerning segregation of duties, records retention, professional review, workplace consultation, incident handling or regulatory reporting that apply to the use case.

10.3 Where a material change in use case, data, model, integration, autonomy or authority boundary may

alter the risk or regulatory status of a deployment, Customer shall reassess the relevant controls before placing the changed use into operational use and shall notify Ongo where Ongo's cooperation is reasonably required.

11. Enforcement and reporting

11.1 Ongo may investigate a suspected violation using information lawfully available to it under the

Agreement and applicable law, and may request information reasonably necessary to assess, contain and remediate the issue.

11.2 Ongo may restrict, disable or suspend affected functionality where reasonably necessary to prevent or

contain material harm, unlawful activity, security compromise, data exposure or a material violation of this AUP. Ongo may act immediately without prior notice where delay would materially increase the risk.

11.3 Where reasonably practicable, Ongo will notify Customer of the restriction or suspension, limit measures to the affected Services or functionality, and cooperate to restore compliant use once the material risk has been addressed.

11.4 Customer shall cooperate reasonably with an investigation or remediation request and shall promptly stop or correct a use that Ongo reasonably identifies as violating this AUP or applicable law.

11.5 Suspected abuse, security issues or unlawful use should be reported using the contact details stated in

the applicable Order Form or Documentation.

12. Changes, interpretation and precedence

12.1 Ongo may make non-material administrative, editorial or clarifying updates to this AUP in accordance with the MSA. A material change that adversely changes Customer's substantive contractual rights or materially restricts an existing permitted use during an active Order Term will apply only as permitted by the Agreement or applicable law.

12.2 If this AUP conflicts with another part of the Agreement, the order of precedence stated in the MSA applies. In particular, an applicable Order Form governs Customer-specific scope, the DPA governs personal-data processing matters within its scope, and the MSA prevails over this AUP unless expressly stated otherwise.

12.3 References to law include that law as amended, replaced or supplemented from time to time. A reference to a regulated, high-impact or prohibited use in this AUP is descriptive and does not itself determine the legal classification of a system or use case.

12.4 If a provision of this AUP is unenforceable in a particular context, the remaining provisions continue to apply to the maximum extent permitted by law, subject to the Agreement.

END OF ACCEPTABLE USE POLICY 2026-27
